IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Hugh L. Brunk

Art Unit: 2134

Application No.: **10/045,654**

Confirmation No.: 1906

Filed: October 26, 2001

For: INCLUDING A METRIC IN A DIGITAL WATERMARK FOR MEDIA AUTHENTICATION

Via Electronic Filing

Examiner: W. Powers

Date: May 15, 2006

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants respectfully request the Board of Patent Appeals and Interferences (hereafter the "Board") to reverse the outstanding final rejection of the pending claims.

This Appeal Brief is in furtherance of a Notice of Appeal filed March 13, 2006 (postcard stamped March 15, 2006). Please charge the fee required under 37 CFR 1.17(f) or any other fee needed to consider this Appeal Brief to our deposit account 50-1071.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventors recorded at Reel 012806, frames 0140-0141, on April 8, 2002.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-9, 11-23, and 25-27 are pending in the present application. Each of these claims stand finally rejected. Please see the Office Action Summary in the final Office Action mailed December 12, 2005 – hereafter referred to as "the final Office Action".

Claims 10 and 24 are canceled without prejudice in the accompanying amendment

STATUS OF AMENDMENTS

An Amendment Accompanying Appeal Brief is filed concurrently herewith. Entry of this amendment is believed proper since it merely cancels claims 10 and 24.

All earlier-filed amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to steganography and data hiding, which can be used to help authenticate media. Please see, e.g., the specification, page 1, paragraph [0002].

One form of steganography is digital watermarking. Digital watermarking may be used to modify media to embed a message or machine-readable code into the media. The media is modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Please see the specification, e.g., at page 1, paragraph [0003].

Claim 25 recites a digital watermarking method including: embedding a digital watermark in a media signal, the digital watermark being designed to be lost or to degrade upon

at least one form of signal processing (see, e.g., semi-fragile and fragile watermarks discussed in paragraphs [0085] starting on page 27, [0039] – [0046] starting on page 11, and [0070] – [0072] starting on page 22); determining a metric for the embedded digital watermark, the metric comprising a benchmark for the embedded digital watermark (see, e.g., paragraphs [0083] staring on page 26 and [0084] on page 27); embedding the metric in the media signal (see, e.g., paragraph [0085] starting on page 27); and embedding data in the media signal, the data indicating how the metric was determined (see, e.g., paragraph [0091] starting on page 29).

Claim 27 recites a method of claim 25 where the embedded data indicates a predetermined metric protocol (see, e.g., paragraphs [0091] starting on page 29 and [0084] – [0085] starting on page 27).

Claim 19 recites a digital watermarking method including: embedding a digital watermark in a media signal (see, e.g., paragraphs [0085] and [0086] starting on page 27 and Fig. 3); analyzing the digital watermark embedded in the media signal to determine a baseline state for the digital watermark (see, e.g., paragraphs [0085] and [0086] starting on page 27 and Fig. 3); embedding first information in the media signal, the first information corresponding to the baseline state of the digital watermark (see, e.g., paragraphs [0087] – [0088] starting on page 28 and Figs. 4a and 4b); and embedding second information in the media signal, the second information corresponding to a rendering channel through which the media signal will be rendered (see, e.g., paragraph [0093] starting on page 30).

Claim 15 recites a digital watermarking method comprising: embedding a digital watermark in a media signal, the digital watermark being designed to be lost or to predictably degrade upon predetermined signal processing; rendering the embedded media signal (see, e.g., semi-fragile and fragile watermarks discussed in paragraphs [0085] starting on page 27, [0039] – [0046] starting on page 11 and [0070] – [0072] starting on page 22); detecting the digital watermark from the rendered embedded media signal (see, e.g., paragraphs [0085] and [0086] starting on page 27 and Fig. 3); generating a metric based on the detected digital watermark (see, e.g., paragraphs [0084] - [0086] starting on page 27 and Fig. 3); and embedding the metric in the embedded media signal (see, e.g., paragraphs [0087] – [0088] starting on page 28 and Figs. 4a

and 4b).

Claim 20 recites a method of claim 19 where the second information comprises color-space information (see, e.g., paragraph [0093] starting on page 30).

Claim 21 recites a method of claim 19 where the second information comprises printer-specific information (see, e.g., paragraph [0093] starting on page 30).

Claim 11 recites a method of determining authenticity of media using a digital watermark embedded in the media, the digital watermark comprising a message (see, e.g., paragraph [0091] starting on page 29). The message includes a measure or characteristic corresponding to the digital watermark signal (see, e.g., paragraphs [0084] on page 27 and [0091] starting on page 29). The method includes: extracting the digital watermark from the media (see, e.g., Fig. 5 and paragraph [0091] starting on page 29); and evaluating the extracted digital watermark in comparison to the message to measure degradation of the digital watermark based on differences between the extracted digital watermark and the message (see, e.g., Fig. 5 and paragraphs [0091] – [0092] starting on page 29).

Claim 13 recites a method of claim 11 where the evaluating includes comparing signal peaks of the digital watermark to signal peak information conveyed by the message (see, e.g., paragraphs [0084] starting on page 27).

Claim 1 recites a method of authenticating media. The media includes a digital watermark having a first metric. The method includes: decoding the digital watermark to obtain the first metric (see, e.g., paragraph [0091] starting on page 29 and Fig. 5), wherein the first metric comprises a measure or characteristic corresponding to the digital watermark (see, e.g., paragraphs [0091] starting on page 29 and [0084] on page 27); analyzing the digital watermark to determine a second metric (see, e.g., paragraph [0091] and [0092] starting on page 29; see also Fig. 5); and comparing the first metric and the second metric to determine whether the media has been altered (see, e.g., paragraph [0091] and [0092] starting on page 29; see also Fig. 5).

Claim 4 recites a method of claim 1 where the first metric and the second metric each comprise a ratio between a selected coefficient and one or more neighboring coefficients (see, e.g., paragraphs [0021] on page 6, [0026] starting on page 7, [0073] on page 23, [0075] on page 24 and [0084] on page 27).

Claim 5 recites a method of claim 1 where the first metric and the second metric each comprise a ratio between a magnitude of a selected coefficient and an average of neighboring coefficients (see, e.g., paragraphs [0021] on page 6, [0026] starting on page 7, [0073] on page 23, [0075] on page 24 and [0084] on page 27).

Claim 6 recites a method of claim 1 where the digital watermark comprises a calibration signal, and wherein the first metric and the second metric are each determined from an analysis of the calibration signal (see, e.g., paragraphs [0008] on page 3, [0084] on page 27 and [0091] starting on page 29).

Claim 7 recites a method of claim 1 where the first metric and the second metric each comprise an evaluation of signal peaks at selected frequency coefficients of the media, where the media has been previously modified to include peaks at the selected frequencies (see, e.g., paragraphs [0021] on page 6, [0026] starting on page 7, [0073] on page 23, [0075] on page 24 and [0084] on page 27 and [0091] starting on page 29).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 15-19 and 22, 23 and 25-27 stand finally rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,330,672 (hereafter "the Shur patent").

2. Claims 20 and 21 stand finally rejected under 35 U.S.C. 103(a) as being unpatentable over the Shur patent in view of U.S. Patent No. 6,366,685 (hereafter "the Takaragi patent").

3. Claims 1 and 4-9 and 11-14 stand finally rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,064,764 (hereafter "the Bhaskaran patent").

ARGUMENT

Appellants respectfully request that the final rejection of the pending claims be reversed since the applied references fail to teach or suggest all of the elements of the pending claims.

Rejections under U.S.C. 102(e) over the Shur patent

Claims 25-26

Claim 25 recites:

25. *A digital watermarking method comprising:*

embedding a digital watermark in a media signal, the digital watermark being designed to be lost or to degrade upon at least one form of signal processing;

determining a metric for the embedded digital watermark, the metric comprising a benchmark for the embedded digital watermark;

embedding the metric in the media signal; and

embedding data in the media signal, the data indicating how the metric was determined.

There are at least three reasons why the final rejection of claim 25 should be reversed.

First, we respectfully submit that the Shur patent at Col. 10, lines 1-11 does not teach or suggest "embedding a digital watermark in a media signal, *the digital watermark being designed to be lost or to degrade upon at least one form of signal processing,*" as implied in the final Office Action. Please see the final Office Action at page 8, lines 8-9.

Some discussion from the specification may be useful.

One example of watermark degrading is seen in the context of a "semi-fragile" digital watermark, as discussed in paragraph [0039] of the present application. The term "semi-fragile" may refer to a digital watermark signal that degrades in response to some types of degradation of the watermarked signal but not others. For example, in some document authentication applications using such a digital watermark, the watermark decoder can determine if the watermark has been scanned and printed or battered by normal usage, potentially while being read with an optical sensor. See, e.g., paragraph [0039].

Another example of watermark degrading is in the context of a "fragile" digital watermark, as discussed in paragraph [0070] of the present application. A digital watermark may be called fragile, e.g., because the strength (or other signal characteristics) of the watermark signal in a copy of the watermarked original object is less than the strength in the original object. See, e.g., paragraph [0070].

(Of course, there are many other examples and implementations that will fall within the scope of claim 25. Thus, citation to specific specification passages should not be viewed as limiting claim scope.)

The final Office Action points to Col. 10, lines 1-11, of the Shur patent as discussing a watermark with a capacity to prevent use of protected content after a predetermined date or number of plays. See the final Office Action at page 8, lines 7-9.

(The actual quote from the Shur patent regarding play control is: "watermark input parametric data may comprise . . . [a] number of permitted plays or other parameter relating to the expiration of any license or lease . . . ." See the Shur patent at Col. 10, lines 1 and 7-8.)

This passage seems primarily focused on data carried by a watermark including a

permitted number of plays for protected content. The permitted number of plays seems provided, perhaps, to control *the protected content* in which a watermark is embedded. There is no discussion of how the permitted number of plays will be used to degrade *the watermark* or cause *the watermark* to become lost.

Indeed, a discussion of restricting use of content based on a number or date carried by a watermark (as cited in the final Office Action) does not teach or suggest designing a watermark to degrade or become lost with signal processing.

Second, we respectfully disagree with the final Office Action's interpretation of the Shur patent at Col. 11, lines 12-24. The final Office Action cites this passage as teaching "generating a metric based on the detected watermark." See the final Office Action at page 8, lines 13-14.

We initially note that the above quoted feature is not even recited in claim 25. Claim 25 recites: "*determining a metric for the embedded digital watermark, the metric comprising a benchmark for the embedded digital watermark.*"

Instead of teaching determining a metric based on an embedded digital watermark the cited passage discusses that decoded watermark information may be operative to deny use of recorded data. See, e.g., Col. 11, lines 15-18. And that a key may be needed based on a level of encryption applied. See, e.g., Col. 11, lines 19-24. And that new data may be added to a digital watermark. See, e.g., Col. 11, lines 13-15.

We fail to understand how this teaches determining a metric for the embedded digital watermark, the metric comprising a benchmark for the embedded digital watermark.

Third, the final Office Action fails to address a limitation of the claim. That is, the final Office Action fails to discuss "embedding data in the media signal, *the data indicating how the metric was determined.*" (emphasis added). See the final Office Action, page 8, lines 6-16.

One example of data indicating how a metric is determined is discussed in the specification at, e.g., paragraph [0091]. If a metric module 18 determines a metric 20 based, e.g., on Fourier characteristics of a watermark orientation signal, a digital watermark may include a payload (or message) indicating how metric 20 was calculated.

Some other examples involving watermark metrics include, e.g., watermark signal strength, a watermark correlation value, a ratio of values, a power ratio between two watermarks, power or energy of a watermark component, a Fourier magnitude peak value, a peak location in a Fourier domain, or location for a watermark component, orientation or synchronization signal strength, Fourier characteristics of the orientation signal, signal gain, a threshold level, signal distortion level, bit-error relationship, e.g., for a watermark message, watermark signal corruption level and/or a signal to noise ratio. See, e.g., the present specification at paragraph [0084].

(Of course many other examples and implementations will fall within the scope of this claim as well. Thus, citation to particular specification passages should not be construed as limiting claim scope.)

The Office has failed to carry its initial burden of rejecting claim 25 by at least neglecting to consider this claim feature (i.e., "embedding data in the media signal, the data indicating how the metric was determined").

Moreover, the cited passages[1] in the Shur patent that are relied upon in the final Office Action are not understood to teach or suggest a combination including, e.g., embedding data in the media signal indicating how the metric was determined.

We respectfully request that the final rejection of claim 25 be reversed.

---

1 See the final Office Action at page 8, lines 6-16, citing the Shur patent at Col. 6, lines 38-45 and lines 61-67; Col. 8, line 56 – Col. 9, line 4; and Col. 10, lines 1-11.

Claim 27

Claim 27 recites:

27. *The method of claim 25 wherein the embedded data indicates a predetermined metric protocol.*

The final Office Action cites the Shur patent at Col. 10, lines 1-11 as teaching the combination recited in claim 27.

We respectfully disagree.

While the cited passage discusses information that can be input to a watermark embedder, e.g., information regarding an encoding algorithm that was used to encode a signal via a perceptual coder, the passage does not discuss information regarding a metric associated with an embedded watermark, let alone a predetermined metric protocol.

We respectfully request that the final rejection of claim 27 be reversed.

Claims 19, 22 and 23

Claim 19 recites:

19. *A digital watermarking method comprising:*

embedding a digital watermark in a media signal;

analyzing the digital watermark embedded in the media signal to determine a baseline state for the digital watermark;

embedding first information in the media signal, the first information corresponding to the baseline state of the digital watermark; and

embedding second information in the media signal, the second information corresponding to a rendering channel through which the media signal will be rendered.

The final rejection of claim 19 should be reversed. A few of the reasons supporting reversal are presented below.

First, the cited passages of the Shur patent do not teach or suggest the combination recited in claim 19. See the final Office Action, page 7, line 11 – page 8, line 2, citing the Shur patent at Col. 6, lines 38-45; Col. 10, lines 1-11 and Col. 11, lines 3-24.

For example, the final Office Action cites an encoding algorithm for digital data in a media stream apparently to teach: "embedding second information in the media signal, *the second information corresponding to a rendering channel through which the media signal will be rendered.*" See the final Office Action at page 8, lines 1-2.

We think there may be a misunderstanding in the final Office Action regarding the meaning of rendering.

Fig. 3 of the present specification provides an example. A media signal is embedded with a watermark via watermark embedder 14. Embedder 14 outputs a digital watermarked media signal 16. The digital watermarked media signal 16 is preferably **rendered** (**e.g., printed, streamed, or broadcast if video or audio**) 17. See, e.g., paragraph [0085] of the present application and Fig. 3.

(Of course many other examples and implementations will fall within the scope of this claim as well. Thus, citation to particular specification passages should not be construed as limiting claim scope.)

Thus, while the cited encoding algorithm may relate generally to an act of embedding, it is not understood to teach or suggest a rendering channel, e.g., a printer, a streaming device or broadcast channel.

Second, we do not understand the cited passages to teach or suggest the interrelationship of the combination recited in claim 19. For example, claim 19 recites that a digital watermark *embedded* in a media is analyzed to determine a baseline state for the digital watermark.

The final Office Action suggests that this baseline feature corresponds to a number of permissible plays carried by a watermark. See the final Office Action at page 7, lines 13-15. So, carrying this position forward, if a number of permissible plays is determined from watermarked media (i.e., as at Col. 11, lines 3-24), information corresponding to this number must then be embedded in the watermarked media signal.

But we do not see any suggestion at the cited passages providing this extracted number back to an embedder for re-embedding. For example, the number of permissible plays might be used to deny use of recorded data (Col. 11, lines 15-18) in a personal disc player. If the personal disc player is denying use, why would it then re-embed a number of permissible plays back into the content? (If the player is denying use, the number of permissible plays seems to be "zero". Why then, would the number (zero) be re-embedded in the media?)

This is but one example of where the interrelationship in the Shur patent – as well as the rejection in the final Office Action – is deficient regarding teaching the combination of claim 19.

We respectfully request that the final rejection of claim 19 be reversed.

Claims 15-18

Claim 15 recites:

15. *A digital watermarking method comprising:*

embedding a digital watermark in a media signal, the digital watermark being designed to be lost or to predictably degrade upon predetermined signal processing;

rendering the embedded media signal;

detecting the digital watermark from the rendered embedded media signal;

generating a metric based on the detected digital watermark; and

embedding the metric in the embedded media signal.

The final rejection of claim 15 should be reversed for at least two reasons.

First, we respectfully submit that the Shur patent at Col. 10, lines 1-11, does not teach or suggest "embedding a digital watermark in a media signal, *the digital watermark being designed to be lost or to predictably degrade upon at least one form of signal processing,"* as implied in the final Office Action. Please see the final Office Action at page 6, lines 5-6 of paragraph 10.

Some discussion from the specification may be useful.

One example of watermark degrading is seen in the context of a "semi-fragile" digital watermark, as discussed in paragraph [0039] of the present application. The term "semi-fragile"

may refer to a digital watermark signal that degrades in response to some types of degradation of the watermarked signal but not others. For example, in some document authentication applications using such a digital watermark, the watermark decoder can determine if the watermark has been scanned and printed or battered by normal usage, potentially while being read with an optical sensor. See, e.g., paragraph [0039].

Another example of watermark degrading is in the context of a "fragile" digital watermark, as discussed in paragraph [0070] of the present application. A digital watermark may be called fragile, e.g., because the strength (or other signal characteristics) of the watermark signal in a copy of the watermarked original object is less than the strength in the original object. See, e.g., paragraph [0070].

(Of course, there are many other examples and implementations that will fall within the scope of claim 15. Thus, citation to specific specification passages should not be viewed as limiting claim scope.)

The final Office Action points to Col. 10, lines 1-11, of the Shur patent as discussing a watermark with a capacity to prevent use of protected content after a predetermined date or number of plays. See the final Office Action at page 6, lines 14-16.

(The actual quote from the Shur patent regarding play control is: "watermark input parametric data may comprise . . . [a] number of permitted plays or other parameter relating to the expiration of any license or lease . . . ." See the Shur patent at Col. 10, lines 1 and 7-8.)

This passage seems primarily focused on data carried by a watermark including a permitted number of plays for protected content. The permitted number of plays seems provided, perhaps, to control *the protected content* in which a watermark is embedded. But there is no discussion of how the permitted number of plays will be used to *degrade the watermark* or cause *the watermark* to become lost upon signal processing.

Indeed, a discussion of restricting use of content based on a number or date carried by a watermark (as cited in the final Office Action) does not teach or suggest designing a watermark to degrade or become lost with signal processing.

Second, we respectfully disagree with the final Office Action's interpretation of the Shur patent at Col. 11, lines 12-24. The final Office Action cites this passage as teaching "generating a metric based on the detected watermark." See the final Office Action at page 7, lines 1-2.

Instead of teaching generating a metric based on a detected watermark the cited passage seems to discuss that decoded watermark information may be operative to deny use of recorded data. See, e.g., Col. 11, lines 15-18. And that a key may be needed based on a level of encryption applied. See, e.g., Col. 11, lines 19-24. And that new data may be added to a digital watermark. See, e.g., Col. 11, lines 13-15.

We fail to understand how this teaches a generating a metric recited in claim 15.

And we respectfully request that the final rejection of claim 15 be reversed.

Rejections under U.S.C. 103(a) over the Shur patent in view of the Takaragi patent

Claim 20

Claim 20 recites:

20. *The method of claim 19, wherein the second information comprises color-space information.*

Recall from claim 19, discussed supra, that the second information is embedded in the media signal. The second information corresponds to a rendering channel through which the media signal will be rendered.

Claim 20 recites that this second information (which is embedded in the media signal) comprises color-space information.

The final Office Action cites the Takaragi patent at Col. 2, lines 35-60 and Col. 4, lines 28-59 as teaching this feature. See the final Office Action at page 10, lines 7-9 of paragraph 12.

But the digital watermark discussed at these passages seems to carry or include copyright information (see Col. 2, lines 42-45) and not color-space information.

Like many print digital watermarking techniques, the digital watermarking in the cited passages of the Takaragi patent is conveyed on a substrate through printing. The printing is by yellow dots (see Col. 2, lines 56-60) or perhaps other colors (see Col. 4, lines 28-59). But printing watermarks with colors does not mean that the digital watermark carries or includes (e.g., via a payload message) color-space information.

We respectfully request that the final rejection of claim 20 be reversed.

Claim 21

Claim 21 recites:

21. *The method of claim 19, wherein the second information comprises printer-specific information.*

Recall from claim 19, discussed supra, that the second information is embedded in the media signal. The second information corresponds to a rendering channel through which the media signal will be rendered.

Claim 21 recites that this second information (which is embedded in the media signal) includes printer-specific information.

The final Office Action cites the Takaragi patent at Col. 2, lines 35-60 and Col. 4, lines 28-59 as teaching this feature. See the final Office Action at page 10, lines 7-9 of paragraph 12.

But the digital watermark discussed at these passages seems to carry or include copyright information (see Col. 2, lines 42-45) and not printer-specific information.

Like in many print digital watermarking techniques, the digital watermarking in the cited passages of the Takaragi patent is conveyed on a substrate through printing. In this case the printing is by yellow dots (see Col. 2, lines 56-60) or perhaps other colors (see Col. 4, lines 28-59). But printing watermarks with colors does not mean that the digital watermark carries or includes (e.g., via a payload message) printer-specific information information.

We respectfully request that the final rejection of claim 21 be reversed.

Rejections under U.S.C. 102(e) over the Bhaskaran patent

Claims 11-12

Claim 11 recites:

11. *A method of determining authenticity of media using a digital watermark embedded in the media, the digital watermark comprising a message, wherein the message comprises a measure or characteristic corresponding to the digital watermark signal, said method comprising:*

extracting the digital watermark from the media; and

evaluating the extracted digital watermark in comparison to the message to measure degradation of the digital watermark based on differences between the extracted digital watermark and the message.

The digital watermark of claim 11 includes a message. The message includes a measure or characteristic corresponding to the digital watermark signal. Support for this feature can be found throughout the specification including, e.g., paragraphs [0083] and [0092]. Once extracted, the message – obtained from the digital watermark – is compared to the digital watermark from which it is extracted from to measure degradation of the digital watermark.

The Bhaskaran patent discusses an image dependent hash (H_1) as a component when crafting a watermark with a private (secret) key. See, e.g., Col. 4, lines 11-16; Col. 5, lines 43-46 and Fig. 2. The watermark is embedded in an image (I).

To verify whether a watermarked image has been tampered with, another (second) hash $(H_2)^2$ is calculated from the watermarked image and the watermark W is extracted from the

---

2 We have chosen to use the notation H_1 and H_2 to simplify our discussion. The Bhaskeran patent refers to both hashes generally as H. We refer to H_1 as a hash (H) that is calculated, e.g., using the Fig. 2 method and then used as a watermark component for embedding in image I. And we refer to H_2 as a hash calculated, e.g., from an embedded image using the Fig. 5 method.

watermark image. See Col. 6, lines 42-45 and Fig. 5.

The second hash (H_2) is compared with the extracted watermark W via a public key. See Col. 6, lines 45-48 and see Fig. 5

But this act does not compare the first hash (H_1) to the watermark. Rather, a different, second hash (H_2) is compared to the watermark.

There may be cases where H_1 and H_2 have the same value – like when there is no tampering of the watermarked image. But even in these cases the comparison is not between a message (e.g., H_1) – included in the watermark – and the watermark itself; and sharing the same value does not mean that H_2 is included in the watermark.

Instead, a Bhaskeran patent comparison suggests a comparison between a component that is not included in a watermark (H_2) with the watermark itself.

We respectfully request that the final rejection of claim 11 be removed.

Claims 13 and 14

Claim 13 recites:

13. *The method of claim 11 wherein the evaluating includes comparing signal peaks of the digital watermark to signal peak information conveyed by the message.*

The final Office Action misquotes the above claim language in its rejection. See page 6, lines 8-10. Thus, it is unclear whether the claim features have been given any consideration.

For example, there is no discussion of *the evaluating including comparing signal peaks of the digital watermark to signal peak information conveyed by the message.*

The cited passage in the Bhaskaran patent (i.e., Col. 3, lines 17-35) is not helpful in this regard.

For example, we do not see a discussion there of signal peak information conveyed by a digital watermark message, or a comparison of such information to the digital watermark.

We respectfully request that the final rejection of claim 13 be reversed.

Claims 1-3, 8 and 9

Claim 1 recites:

1. *A method of authenticating media, the media comprising a digital watermark including a first metric, said method comprising:*

decoding the digital watermark to obtain the first metric, wherein the first metric comprises a measure or characteristic corresponding to the digital watermark;

analyzing the digital watermark to determine a second metric; and

comparing the first metric and the second metric to determine whether the media has been altered.

A digital watermark is decoded to obtain a first metric. The first metric comprises a measure or characteristic corresponding to the digital watermark.

The digital watermark is analyzed to determine a second metric to compare with the first metric.

Claim 1 compares two metrics associated with the watermark – a first metric decoded from the watermark and a second metric determined from the watermark.

The Bhaskaran patent discusses an image dependent hash (H_1) as a component when crafting a watermark with a private (secret) key. See, e.g., Col. 4, lines 11-16; Col. 5, lines 43-46 and Fig. 2. The watermark is embedded in an image (I).

To verify whether a watermarked image has been tampered with, another (second) hash (H_2)[3] is calculated from the image and the watermark W is extracted from the image. See Col. 6, lines 42-45 and Fig. 5.

---

3 We have chosen to use the notation H_1 and H_2 to simplify our discussion. The Bhaskeran patent refers to both hashes generally as H. We refer to H_1 as a hash (H) that is calculated, e.g., using the Fig. 2 method and then used as a watermark component for embedding in image I. And we refer to H_2 as a hash calculated, e.g., from an embedded image using the Fig. 5 method.

The second hash (H_2) is compared with the extracted watermark W via a public key. See Col. 6, lines 45-48 and see Fig. 5

But this act does not compare the first metric - decoded from the watermark - to a second metric - determined based on analyzing the watermark.

Rather, a second hash (H_2) obtained from the image is compared to the watermark embedded in the image.

We respectfully request that the final rejection of claim 11 be removed.

Claim 4

Claim 4 recites:

4. *The method of claim 1 wherein the first metric and the second metric each comprise a ratio between a selected coefficient and one or more neighboring coefficients.*

The final Office Action misstates the above claim language in its rejection. See page 5, lines 7-9. Thus, it is unclear whether the claim features have been given any consideration.

For example, there is no discussion of a ratio between a selected coefficient and one or more neighboring coefficients.

The cited passage in the Bhaskaran patent (i.e., Col. 4, lines 11-15) is not helpful in this regard. That passage seems to discuss computing a hash for use in creating a watermark via a secret key. We do not see a discussion of a first and second metric each comprising a ratio between a selected coefficient and one or more neighboring coefficients, at the cited passages.

We respectfully request that the final rejection of claim 4 be reversed.

Claim 5

Claim 5 recites:

5. *The method of claim 1 wherein the first metric and the second metric each comprise a ratio between a magnitude of a selected coefficient and an average of neighboring coefficients.*

The final Office Action misstates the above claim language in its rejection. See page 5, lines 7-9. Thus, it is unclear whether the claim features have been given any consideration.

For example, there is no discussion of a ratio between a magnitude of a selected coefficient and an average of neighboring coefficients.

The cited passage in the Bhaskaran patent (i.e., Col. 4, lines 11-15) is not helpful in this regard. That passage seems to discuss computing a hash for use in creating a watermark via a secret key.

We do not see a discussion of a first metric and second metric each comprising a ratio between a magnitude of a selected coefficient and an average of neighboring coefficients at the cited passages.

We respectfully request that the final rejection of claim 5 be reversed.

Claim 6

Claim 6 recites:

6. *The method of claim 1 wherein the digital watermark comprises a calibration signal, and wherein the first metric and the second metric are each determined from an analysis of the calibration signal.*

The final Office Action discusses entropy coding for these claim features. See the final Office Action, page 5, lines 10-12.

Perhaps the final Office Action intends entropy coding to correspond to the calibration signal in claim 6?

But even if the "entropy coding" is mapped to the calibration signal recited in claim 6, the Bhaskaran patent does not then determine first and second metrics from an analysis of the entropy coding. Rather, the cited passage (Col. 6, lines 24-31) seems to suggest that entropy coding of compressed data is undone, avoiding the de-zip-zagging, dequantization, and IDCT steps needed for full decompression. See Col. 6, lines 25-27. This results in a representation of non-zero quantized coefficients along with their location in the zig-zag order. See Col. 6, lines

27-31.

We respectfully request that the final rejection of claim 6 be reversed.

Claim 7

Claim 7 recites:

7. *The method according to claim 1 wherein the first metric and the second metric each comprise an evaluation of signal peaks at selected frequency coefficients of the media, where the media has been previously modified to include peaks at the selected frequencies.*

The final Office Action misstates the above claim language in its rejection. See page 5, lines 13-15. Thus, it is unclear whether the claim features have been given any consideration.

For example, there is no discussion of a first metric and a second metric each comprising an evaluation of signal peaks at selected frequency coefficients of the media, where the media has been previously modified to include peaks at the selected frequencies.

The cited passage in the Bhaskaran patent (i.e., Col. 3, lines 18-24) is not helpful in this regard.

We respectfully request that the final rejection of claim 7 be reversed.

CONCLUSION AND REQUEST FOR REVERSAL

The applied references fail to teach all of the limitations of the pending claims. (Other deficiencies of the art need not be further belabored at this time.) As such, the claims are patentable over the cited references. Appellants respectfully request that the Board reverse the final rejection of the pending claims.

Respectfully submitted,

Date: May 15, 2006

DIGIMARC CORPORATION

Customer No.: 23735

By 

Telephone: 503-469-4685
FAX: 503-469-4777

Steven W. Stewart
Registration No. 45,133

CLAIMS APPENDIX

1. (previously presented): A method of authenticating media, the media comprising a digital watermark including a first metric, said method comprising:

decoding the digital watermark to obtain the first metric, wherein the first metric comprises a measure or characteristic corresponding to the digital watermark;

analyzing the digital watermark to determine a second metric; and

comparing the first metric and the second metric to determine whether the media has been altered.

2. (original): The method of claim 1 wherein an alteration comprises at least one of scanning, printing, editing, digital capture and photocopying the media.

3. (original): The method of claim 2 wherein the alteration is determined if the first and second metrics do not relate.

4. (original): The method of claim 1 wherein the first metric and the second metric each comprise a ratio between a selected coefficient and one or more neighboring coefficients.

5. (original): The method of claim 1 wherein the first metric and the second metric each comprise a ratio between a magnitude of a selected coefficient and an average of neighboring coefficients.

6. (original): The method of claim 1 wherein the digital watermark comprises a calibration signal, and wherein the first metric and the second metric are each determined from an analysis of the calibration signal.

7. (original): The method according to claim 1 wherein the first metric and the second metric each comprise an evaluation of signal peaks at selected frequency coefficients of the media, where the media has been previously modified to include peaks at the selected frequencies.

8. (original): The method of claim 1 wherein the media comprises at least one of a product tag, product label, identification card, identification document, image, photograph, picture, passport, license, stock certificate, bond certificate, deed, legal document, company logo, paper, product packaging, audio signal, video signal, sport card, trading card, digital signal, game card, advertisement, printed media, envelope, letterhead, stationary, book, sticker, business card, fabric and clothing.

9. (original): The method according to claim 1 wherein said first metric comprises at least one of a power ratio, power signature of the digital watermark, energy level, threshold amount, color space information, spot color information, acceptable degradation level and printer type.

10. canceled.

11. (previously presented): A method of determining authenticity of media using a digital watermark embedded in the media, the digital watermark comprising a message, wherein the message comprises a measure or characteristic corresponding to the digital watermark signal, said method comprising:

extracting the digital watermark from the media; and

evaluating the extracted digital watermark in comparison to the message to measure degradation of the digital watermark based on differences between the extracted digital watermark and the message.

12. (previously presented): The method of claim 11, wherein the digital watermark message comprises a first metric and the evaluating generates a second metric based on an analysis of the extracted digital watermark, the first metric being compared to the second metric to measure degradation of the extracted digital watermark.

13. (previously presented): The method of claim 11 wherein the evaluating includes comparing signal peaks of the digital watermark to signal peak information conveyed by the message.

14. (original): The method of claim 13, wherein the signal peaks comprise frequency domain peaks.

15. (previously presented): A digital watermarking method comprising:

embedding a digital watermark in a media signal, the digital watermark being designed to be lost or to predictably degrade upon predetermined signal processing;

rendering the embedded media signal;

detecting the digital watermark from the rendered embedded media signal;

generating a metric based on the detected digital watermark; and

embedding the metric in the embedded media signal.

16. (previously presented): The method of claim 15 wherein said rendering comprises at least one of printing, broadcasting and streaming.

17. (previously presented): The method of claim 15 wherein the metric is embedded in the embedded media signal so as to be part of the digital watermark.

18. (previously presented): The method of claim 15 wherein the metric is embedded in the embedded media signal as a second digital watermark.

19. (previously presented): A digital watermarking method comprising:

embedding a digital watermark in a media signal;

analyzing the digital watermark embedded in the media signal to determine a baseline state for the digital watermark;

embedding first information in the media signal, the first information corresponding to the baseline state of the digital watermark; and

embedding second information in the media signal, the second information corresponding to a rendering channel through which the media signal will be rendered.

20. (previously presented): The method of claim 19, wherein the second information comprises color-space information.

21. (previously presented): The method of claim 19, wherein the second information comprises printer-specific information.

22. (previously presented): The method of claim 19, wherein the second information comprises at least rendering device information.

23. (previously presented): The method of claim 19, wherein prior to said analyzing, said method further comprises rendering the embedded media signal, and said analyzing comprises analyzing the rendered media signal to determine a baseline state for the digital watermark embedded therein.

24. canceled.

25. (previously presented): A digital watermarking method comprising:

embedding a digital watermark in a media signal, the digital watermark being designed to be lost or to degrade upon at least one form of signal processing;

determining a metric for the embedded digital watermark, the metric comprising a benchmark for the embedded digital watermark;

embedding the metric in the media signal; and

embedding data in the media signal, the data indicating how the metric was determined.

26. (previously presented): The method of claim 25 further comprising encrypting the data prior to embedding the data in the media signal.

27. (previously presented): The method of claim 25 wherein the embedded data indicates a predetermined metric protocol.

EVIDENCE APPENDIX

(No Evidence)

RELATED PROCEEDINGS APPENDIX

(No Related Proceedings)